Properties of subspace subcodes of optimum codes in rank metric

E. M. Gabidulin[*]and P. Loidreau[†]

February 1, 2008

Abstract

Maximum rank distance codes denoted MRD-codes are the equivalent in rank metric of MDS-codes. Given any integer q power of a prime and any integer n there is a family of MRD-codes of length n over $GF(q^n)$ having polynomial-time decoding algorithms. These codes can be seen as the analogs of Reed-Solomon codes (hereafter denoted RS-codes) for rank metric. In this paper their subspace subcodes are characterized. It is shown that hey are equivalent to MRD-codes constructed in the same way but with smaller parameters. A specific polynomial-time decoding algorithm is designed. Moreover, it is shown that the direct sum of subspace subcodes is equivalent to the direct product of MRD-codes with smaller parameters. This implies that the decoding procedure can correct errors of higher rank than the error-correcting capability. Finally it is shown that, for given parameters, subfield subcodes are completely characterized by elements of the general linear group $\mathrm{GL}_n(GF(q))$ of non-singular q-ary matrices of size n.

1 Introduction

This work was initiated due to the great similarity between RS-codes and the family of MRD-codes initially published in [6]. It was also due to the constant interest of research in the study of codes derived from RS-codes, particularly subfield subcodes of RS-codes and more recently subspace subcode of RS-codes. Subspace subcodes or subgroup subcodes consist of the set of codewords whose components belong to a specific subspace or subgroup

[*] gab@pop3.mipt.ru

[†] Pierre.Loidreau@ensta.fr

of the additive group alphabet of the code [11]. These particular subcodes are in general not linear but simply *additive*.

In the case of RS-codes abundant literature is available especially on subfield subcodes, that is when the considered subspace is a subfield of the alphabet field. Indeed RS-codes and derived families (GRS-codes for instance) form a very popular family of codes. Some of the most studied codes can be seen as particular subfield subcodes of RS-codes or GRS-codes (Alternant codes, binary Goppa codes and BCH-codes for example) [9, 15]. In cryptography also they play an important role, for instance in McEliece public-key cryptosystem which uses in its design the family of binary Goppa codes [16].

Concerning more general subcodes like subspace subcodes of RS-codes, research on the subject was initiated in 1992 [22]. One of the objects of the research is to provide longer character-oriented codes than RS-codes, that is to build codes with good parameters, but whose symbol length is controlled, smaller than the extension degree of the field.

In general however, even the simple question of the dimension of the subfield subcodes and their exact minimum distance remains open, although some bounds are derived from bounds or equalities on parameters of the parent RS-codes [5, 23, 1]. Concerning subspace subcodes, the same questions arise and again some bounds are obtained from RS-codes. More specifically, it was shown that their cardinality depended on the structure of the subspace of the alphabet field, relatively to the action of the Frobenius automorphism [17, 10].

An additional problem the user of subspace subcode must cope with is the encoding of the code. Since these codes are not linear but simply additive, there is no generator matrix and therefore no systematic procedure can be built. In the case of *bit shortened RS-codes* a systematic encoding procedure was designed [22]. In a more general case of MDS codes an fast but not completely optimal procedure was designed in [24]. The principle consist of considering a codeword of length n over $GF(q^n)$ as an $m \times n$ q-ary matrix and by putting information on some subblock of the matrix, parities on some other block and some relations must be satisfied on the remaining positions. However since only lower bound on the cardinality of the codes are known, these encoding procedures do not take into account the additional bits that could be encoded and therefore are not optimal.

In the same way as RS-codes in Hamming metric the family of MRD-codes constructed in [6] can be efficiently used for decoding in rank metric, for example, whenever the errors occur along some rows or columns of arrays, which happens along tapes [21, 20]. Moreover, properties of rank metric have interesting cryptographic applications, in particular in the design of McEliece-like cryptosystems, see [8, 4]. Namely, for the same set of parameters general purpose decoding algorithms in rank metric have a much higher complexity compared to general purpose decoding algorithms for Hamming metric [3, 18, 2]. Therefore the MRD-codes or codes derived from MRD-codes can be of interest in designing cryptosystems. Several fast polynomial-time decoding algorithm up to the error-correction capability exist whose design that all have their equivalent in decoding RS-codes. There are Euclidian and Berlekamp Massey like algorithms [6, 7, 21, 20] as well as Welch-Berlekamp like algorithms, [14, 13].

Let $GF(q)$ be the base field and $GF(q^n)$ be an extension field of degree n of $GF(q)$. In the following we will indifferently consider $GF(q^n)$ as the field or the n-dimensional vector space over $GF(q)$. We recall properties of rank metric, [6].

Definition 1 (Rank of a vector)

Let $\mathbf{e} = (e_1, \ldots, e_n) \in GF(q^n)^n$. The rank over $GF(q)$ of $\mathbf{e}$ is the rank of the $n \times n$ q-ary matrix obtained by extending every component e_i over a basis of $GF(q^N)/GF(q)$. It is denoted $Rk(\mathbf{e}|GF(q))$.

The rank over $GF(q)$ of vector $\mathbf{e}$ is denoted in the following by $\mathrm{Rk}(\mathbf{e})$. We define $[i] \overset{def}{=} q^i$, when $i \geq 0$ and $[i] \overset{def}{=} q^{n+i}$ when $i < 0$.

A $[n, k, d]$-code over the field $GF(q^n)$ has generator matrix

$$\mathbf{G} = \begin{pmatrix} g_1 & \cdots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}, \tag{1.1}$$

where $g_1, \ldots, g_n \in GF(q^n)$ are linearly independent elements of $GF(q^n)/GF(q)$. A parity-check matrix $\mathbf{H}$ of the code has the same structure as $\mathbf{G}$ that is

$$\mathbf{H} = \begin{pmatrix} h_1 & \cdots & h_n \\ \vdots & \ddots & \vdots \\ h_1^{[d-2]} & \cdots & h_n^{[d-2]} \end{pmatrix}, \tag{1.2}$$

for $h_1, \ldots, h_n \in GF(q^n)$ linearly independent over $GF(q)$. The h_i's of such codes can be easily found from the g_i's [6].

The code $\mathcal{G}$ with parity-check matrix $\mathbf{H}$ or generator matrix $\mathbf{G}$ has minimum rank distance exactly $d = n - k + 1$. This code satisfies the Singleton like equality for rank metric, and since Hamming metric is thinner than rank metric, this implies equally that it is a MDS code. There are several polynomial-time decoding algorithms decoding these codes up to their error-correction capability [6, 7, 21, 20, 13]. It is remarkable to note that these algorithms are can be retranscripted from the algorithms decoding Reed-Solomon codes by replacing the notion of polynomial by the notion of linearized polynomials, that is inherent to the very definition of rank metric. Such similarity and such strong structure raises the natural question of the structure of subcodes of MRD-codes.

The goal of this paper is to show that, despite the fact that the family of MRD-codes with parity-check matrix (1.2) are very similar to RS-codes, they are much more structured, and all the question concerning the dimension of subspace subcodes, their exact minimum rank distance and the design of specific encoding-decoding procedures can be solved quite simply.

The paper is organized as follows: In a first part we show that subspace subcodes of a $(n, k = n-d+1, d)$ MRD-code over a m-dimensional subspace of $GF(q^n)$ can be put in one-to-one correspondence with a $(m, k' = m - d+1, d)$ MRD-code over $GF(q^n)$. More specifically we construct a bijective rank preserving $GF(q)$-linear mapping between the two codes. The mapping enables to build specific encoding and decoding procedures.

In a second part we are interested in subcodes obtained from the direct sum of subspace subcodes and we show that it is possible to construct a rank-preserving mapping putting these subcodes in bijection with the direct product of MRD-codes. In that case we show that it is sometimes possible to correct beyond the error-correcting capability of the codes.

In a third part we deal with subfield subcodes of MRD-codes. We show that they are similar to the direct product of MRD-codes over the subfield, and that up to the action of the general linear group $\mathrm{GL}_n(GF(q))$ on the components of the codewords, they can be uniquely defined. This implies in particular that results from second part apply and that sometimes it is possible to decode them beyond the error-correcting capability of the codes.

2 Subspace subcodes of rank codes

Let $\mathcal{G}$ be the code with generator matrix (1.1) and parity-check matrix (1.2). Consider V_m a m-dimensional subspace of $GF(q^n)$. Let

$$(\mathcal{G}|V_m) \overset{def}{=} \{\mathbf{c} = (c_1, \dots, c_n) \in \mathcal{G} \mid c_j \in V_m,\ j = 1, \dots, n\}$$

Definition 2

$(\mathcal{G}|V_m)$ is called subspace subcode of $\mathcal{G}$ over V_m.

$(\mathcal{G}|V_m)$ is formed of the codewords whose components lie in the alphabet formed by the subspace V_m. In a first section we construct a mapping between $(\mathcal{G}|V_m)$ and a so-called parent code $\mathcal{LG}(V_m)$. This code is MRD and we show that the mapping is bijective, preserves $GF(q)$-linearity and the rank. In a second part we describe encoding and decoding procedures for subspace subcodes.

2.1 Characterization of subspace subcodes

Let $\mathbf{c} = (c_1, \ldots, c_n)$, $c_j \in V_m$ for all j. Let $\mathbf{b} = (\beta_1, \ldots, \beta_m)$ be a basis of V_m. Vector $\mathbf{c}$ has a unique decomposition under the form

$$\mathbf{c} = \mathbf{b}U = (\beta_1, \ldots, \beta_m)U, \tag{2.3}$$

where $U = (U_{ij})_{i=1,j=1}^{m,n} \in GF(q)^{m \times n}$. Vector $\mathbf{c}$ is a codeword if and only if it satisfies the parity-check equations

$$\mathbf{c}\mathbf{H}^T = (\beta_1, \ldots, \beta_m)U\mathbf{H}^T = \mathbf{0}. \tag{2.4}$$

Hence $(\mathcal{G}|V_m)$ is characterized by the *fixed* basis $\mathbf{b} = (\beta_1, \ldots, \beta_m)$ and by the set of $m \times n$ matrices U with coefficients in $GF(q)$ satisfying condition (2.4). Solving (2.4) is equivalent to solving

$$(\beta_1, \ldots, \beta_m)\begin{pmatrix} v_1 & \cdots & v_1^{[d-2]} \\ \vdots & \ddots & \vdots \\ v_m & \cdots & v_m^{[d-2]} \end{pmatrix} = \mathbf{0}, \tag{2.5}$$

where

$$(v_1, \ldots, v_m) = (h_1, \ldots, h_n)U^t. \tag{2.6}$$

Given any vector $(v_1, \ldots, v_m) \in GF(q^n)^m$, there exists a unique $m \times n$ q-ary matrix U such that $(v_1, \ldots, v_m) = (h_1, \ldots, h_n)U^t$. The ith column of U is given by the vector obtained from the representation of v_i over the basis $(h_1, \ldots, h_n)$.

Condition (2.5) is equivalent to

$$(v_1, \ldots, v_m)\begin{pmatrix} \beta_1^{[n]} & \ldots & \beta_1^{[n-d+2]} \\ \vdots & \ddots & \vdots \\ \beta_m^{[n]} & \ldots & \beta_m^{[n-d+2]} \end{pmatrix} = \mathbf{0}. \tag{2.7}$$

Since $\beta_1, \ldots, \beta_m$ are linearly independent, equation (2.7) implies that $\mathbf{v} = (v_1, \ldots, v_m)$ is a codeword of a $GF(q^n)$-linear MRD-code with parameters $[m, m-d+1, d]$. The code with parity-check matrix

$$\mathbf{H}_{V_m} = \begin{pmatrix} \beta_1^{[n]} & \cdots & \beta_m^{[n]} \\ \vdots & \ddots & \vdots \\ \beta_1^{[n-d+2]} & \cdots & \beta_m^{[n-d+2]} \end{pmatrix} \tag{2.8}$$

is denoted $\mathcal{LG}(V_m)$

Definition 3 (Parent Code)
The code $\mathcal{LG}(V_m)$ is called the parent code of $(\mathcal{G}|V_m)$.

We now prove the following proposition establishing that any subspace subcode of a MRD-code of full length is uniquely characterized by a MRD-code with the same minimum distance but with smaller parameters.

Proposition 1
Let $\mathbf{b} = (\beta_1, \ldots, \beta_m)$ be a basis of V_m over $GF(q)$, and let $\mathbf{h} = (h_1, \ldots, h_n)$ be the vector defined in equation (1.2). The mapping

$$\begin{array}{rcl} f_{\mathbf{b}} : \ V_m^n & \rightarrow & GF(q^n)^m \\ \mathbf{c} = \mathbf{b}U & \mapsto & f_{\mathbf{b}}(\mathbf{c}) = \mathbf{h}U^t \end{array}$$

satisfies the following properties

1. *$f_{\mathbf{b}}$ is a $GF(q)$-linear bijective mapping.*

2. *$f_{\mathbf{b}}$ preserves the rank of vectors over $GF(q)$, that is $Rk\left(f_{\mathbf{b}}(\mathbf{c})|GF(q)\right) = Rk(\mathbf{c}|GF(q))$.*

3. *$f_{\mathbf{b}}\left(\mathcal{G}|V_m\right) = \mathcal{LG}(V_m)$.*

4. *$f_{\mathbf{b}}$ and $f_{\mathbf{b}}^{-1}$ can be computed in nm multiplications in $GF(q)$ and n additions in $GF(q^n)$.*

Proof.

1. Since $h_1, \ldots, h_n$ are linearly independent over $GF(q)$, it follows that $f_{\mathbf{b}}$ is a bijection. Let $\mathbf{c} = \mathbf{b}U$ and $\mathbf{d} = \mathbf{b}V$ be vectors of V_m^n. By definition of $f_{\mathbf{b}}$, we have $f_{\mathbf{b}}(\mathbf{c} + \mathbf{d}) = \mathbf{b}(U + V) = f_{\mathbf{b}}(\mathbf{c}) + f_{\mathbf{b}}(\mathbf{d})$.

2. Let $\mathbf{c} = \mathbf{b}U$. Since $\beta_1, \ldots, \beta_m$ are linearly independent, we have that $\mathrm{Rk}(\mathbf{c}|GF(q)) = \mathrm{Rk}(U)$, where $\mathrm{Rk}(U)$ is the rank of matrix U. Moreover, since $f_{\mathbf{b}}(\mathbf{c}) = \mathbf{h}U^t$, and $h_1, \ldots, h_n$ are linearly independent,we have that

$$\mathrm{Rk}(f_{\mathbf{b}}(\mathbf{c})|GF(q)) = \mathrm{Rk}(U^t) = \mathrm{Rk}(U) = \mathrm{Rk}(\mathbf{c}|GF(q))$$

3. The fact that $f_{\mathbf{b}}\left(\mathcal{G}|V_m\right) = \mathcal{LG}(V_m)$, follows directly from the definition of mapping $f_{\mathbf{b}}$.

4. Any vector of V_m^n is given by a q-ary $m \times n$ matrix U. Therefore, computing $f_{\mathbf{b}}$ is merely computing the product of vector $\mathbf{h} = (h_1, \ldots, h_n)$ by matrix U. This can be done in nm multiplications in $GF(q)$ and n additions in $GF(q^m)$. Conversely, computing $f_{\mathbf{b}}^{-1}(v_1, \ldots, v_m)$ corresponds to finding the unique q-ary matrix U such that $(v_1, \ldots, v_m) = (h_1, \ldots, h_n)U^t$, and then compute $\mathbf{b}U$.

We deduce the following corollary.

Corollary 1
$(\mathcal{G}|V_m)$ is a (n, M, D)-additive code, where

- $D = d$,
- $M = q^{n(m-D+1)}$.

Both statements of the corollary imply that $(\mathcal{G}|V_m)$ is optimal for the rank metric [19].

2.2 Coding and decoding of subspace subcodes

Thanks to the mapping $f_{\mathbf{b}}$ described in proposition 1, we design an efficient encoding procedure for subspace subcodes of MRD-codes. From Corollary 1 the number of q-ary digits that can be encoded is equal to $n(m-d+1)$. Hence any information vector can be considered as a vector of length $(m-d+1)$ over $GF(q^n)$.

Let $\mathbf{x} = (x_1, \ldots, x_{m-d+1}) \in GF(q^n)^{m-d+1}$ be an information vector. Let $\mathbf{G}_{V_m}$ be a generator matrix of the parent code $\mathcal{LG}(V_m)$.

The encoding procedure is the following:

1. Encoding in the parent code: Compute $\mathbf{y} = \mathbf{x}\mathbf{G}_{.}V_m \in \mathcal{LG}(V_m)$;

2. Transferring in the subcode: Compute $\mathbf{c} = f_{\mathbf{b}}^{-1}(\mathbf{y})$.

The complexity of the encoding procedure consists of $(m-d+1)m$ multiplications in $GF(q^n)$ if we neglect the operations over the base field $GF(q)$.

Let $\mathbf{y} = \mathbf{c}+\mathbf{e}$ be a received vector where $\mathbf{c} \in (\mathcal{G}|V_m)$ and $\mathbf{e}$ has coefficients in V_m and rank $t \leq \lfloor (d-1)/2 \rfloor$. There are two manners of decoding:

- In the code $\mathcal{G}$ by using the standard decoding algorithms for $\mathcal{G}$. The complexity is $\approx (d-1+t)n + t^3$ multiplications in $GF(q^n)$ if we take the decoding algorithm described in [7].

- By decoding in the parent code $\mathcal{LG}(V_m)$: We have $f_{\mathbf{b}}(\mathbf{y}) = f_{\mathbf{b}}(\mathbf{c}) + f_{\mathbf{b}}(\mathbf{e})$, where $f_{\mathbf{b}}(\mathbf{c}) \in \mathcal{LG}(V_m)$, and $\mathrm{Rk}(f_{\mathbf{b}}(\mathbf{e})|GF(q)) = t$. Therefore, by correcting $f_{\mathbf{b}}(\mathbf{y})$ in $\mathcal{LG}(V_m)$, one recovers $f_{\mathbf{b}}(\mathbf{c})$ and $f_{\mathbf{b}}(\mathbf{e})$ and by computing the inverse function one gets $\mathbf{c}$ and $\mathbf{e}$. The complexity of the algorithm is $\approx (d-1)m + tn + t^3$ multiplications in $GF(q^n)$.

2.3 Direct sum of subspace subcodes

In the previous section, we showed that subspace subcodes of MRD-codes are in some sense isomorphic to MRD-codes of smaller length. From subspace subcodes, we build codes corresponding to the direct sum of subspace subcodes. The mapping $f_{\mathbf{b}}$ can be extended to this direct sum.

Consider a sequence $V_{m_1}, \ldots, V_{m_u}$ of subspaces of $GF(q^m)$ of dimensions m_i that two-by-two do not intersect except on the zero-vector (this implies in particular that $\sum_{i=1}^{u} m_i \leq n$). For every subspace V_{m_i} we fix a basis $\mathbf{b}_i$.

As before $(\mathcal{G}|V_{m_i})$ denotes the subspace subcode of the code $\mathcal{G}$ restricted to vectors with coordinates in V_{m_i}. Let

$$\mathcal{M} \overset{def}{=} (\mathcal{G}|V_{m_1}) \oplus \cdots \oplus (\mathcal{G}|V_{m_u}) \subset \mathcal{G}$$

be the subcode of $\mathcal{G}$ consisting of the direct sum of the subspace subcodes $(\mathcal{G}|V_{m_i})$, that is

$$\mathcal{M} = \{\mathbf{c} = \mathbf{c}_1 + \cdots + \mathbf{c}_u \mid \mathbf{c}_1 \in (\mathcal{G}|V_{m_1}), \ldots, \mathbf{c}_u \in (\mathcal{G}|V_{m_u})\}. \qquad (2.9)$$

We define the mapping $f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}$ from restricted mappings $f_{\mathbf{b}_i}$ as defined in proposition 1:

$$\begin{array}{rcl} V_{m_1}^n \oplus \cdots \oplus V_{m_u}^n & \rightarrow & GF(q^n)^{m_1} \times \cdots GF(q^n)^{m_u} \\ \mathbf{c} = \mathbf{c}_1 + \cdots + \mathbf{c}_u & \mapsto & f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}(\mathbf{c}) = (f_{\mathbf{b}_1}(\mathbf{c}_1), \ldots, f_{\mathbf{b}_u}(\mathbf{c}_u)) \end{array}$$

Proposition 2

$f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}$ is $GF(q)$-linear, bijective and preserves the rank.

PROOF.

$GF(q)$-linearity and bijectivity come from the fact that $f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}$ is a direct product of $GF(q)$-linear, bijective mappings.

Concerning the rank property, any vector $\mathbf{c} \in V_{m_1}^n \oplus \cdots \oplus V_{m_u}^n$ can be uniquely written under the form

$$\mathbf{c} = \mathbf{b}_1 U_1 + \cdots + \mathbf{b}_u U_u,$$

where U_i's are nm_i q-ary matrices. This can be rewritten under the form

$$\mathbf{c} = (\mathbf{b}_1, \ldots, \mathbf{b}_u) \begin{pmatrix} U_1 \\ \vdots \\ U_u \end{pmatrix}.$$

Since, for $i = 1, \ldots, u$ vector spaces V_i form a direct sum, this implies that the components of vector $(\mathbf{b}_1, \ldots, \mathbf{b}_u)$ are linearly independent over $GF(q)$. Therefore the rank of $\mathbf{c}$ over $GF(q)$ is equal to the rank of matrix

$$\mathcal{U} = \begin{pmatrix} U_1 \\ \vdots \\ U_u \end{pmatrix}.$$

Therefore, since $f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}(\mathbf{c}) = \mathbf{h}\mathcal{U}^t$, we have

$$\mathrm{Rk}\left(f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}(\mathbf{c})|GF(q)\right) = \mathrm{Rk}(\mathbf{c}|GF(q)).$$

Let $\mathcal{LG}(\mathcal{M})$ be the code with parity-check matrix,

$$\mathbf{H}(\mathcal{M}) = \begin{bmatrix} \mathbf{H}_{V_{m_1}} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathbf{H}_{V_{m_u}} \end{bmatrix}. \tag{2.10}$$

We prove the following proposition

Proposition 3 *$f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}(\mathcal{M}) = \mathcal{LG}(\mathcal{M})$.*

Proof.

Let $\mathbf{H}$ be the parity-check matrix of $\mathcal{G}$ under the form (1.2). Let $\mathbf{c} = \mathbf{c}_1 + \cdots + \mathbf{c}_u \in \mathcal{M}$. Since for all $i = 1, \ldots, u$, $\mathbf{c}_i \in (\mathcal{G}|V_{m_i})$ we have for all $i = 1, \ldots, u$, $\mathbf{c}_i\mathbf{H} = 0$. This is equivalent to $f_{\mathbf{b}_i}(\mathbf{c}_i)\mathbf{H}_{V_{m_i}} = 0$, for all $i = 1, \ldots, u$.

For this reason $\mathcal{LG}(\mathcal{M})$ is called parent code of $\mathcal{M}$. As it is also a direct product of MRD-codes with smaller parameters, we deduce the following corollary.

Corollary 2 *$\mathcal{M}$ is a (n, M, D)-code, where*

- $M = q^{n\sum_{i=1}^{u}(m_i-(d-1))}$.

- $D = d$.

From $f_{(\mathbf{b}_1,\dots,\mathbf{b}_u)}$ we deduce efficient specific encoding and decoding procedures for code $\mathcal{M}$.

Let $\mathbf{x}$ be q^n-ary vector of length $\sum_{i=1}^u m_i - u(d-1)$.

1. Vector $\mathbf{x}$ is first divided into u blocks $\mathbf{x}_i$ each of length $m_i - d + 1$.
2. Any subvector $\mathbf{x}_i$ is encoded into $\mathbf{c}_i \in (\mathcal{G} \mid V_{m_i})$, using the procedure described in section 2.2 with mapping $f_{\mathbf{b}_i}$.
3. The encoded codeword is $\mathbf{c} = \mathbf{c}_1 + \cdots + \mathbf{c}_u \in \mathcal{M}$.

Since $\mathcal{LG}(V_m)$ can be decomposed into a direct product of subspace subcodes, we show that we can go further in the decoding and that it is sometimes possible to decode beyond the error-correcting capability $C \overset{def}{=} \lfloor (d-1)/2 \rfloor$ of the code. Let the received vector

$$\mathbf{y} = \mathbf{c} + \mathbf{e} \in V_{m_1}^n \oplus \cdots \oplus V_{m_u}^n,$$

where $\mathbf{c} \in \mathcal{M}$ and $\mathbf{e}$ is some error-vector of rank less than t. Let $\mathbf{y}_i$ be the projection of $\mathbf{y}$ on subspace V_{m_i}. We have the following set of equations

$$\begin{cases} \mathbf{y}_1 = \mathbf{c}_1 + \mathbf{e}_1, \ \mathbf{c}_1 \in (\mathcal{G}|V_{m_1}), \\ \vdots \\ \mathbf{y}_u = \mathbf{c}_u + \mathbf{e}_u, \ \mathbf{c}_u \in (\mathcal{G}|V_{m_u}). \end{cases}$$

where, for all $i = 1, \dots, u$ the rank of $\mathbf{e}_i$ over $GF(q)$ is less or equal to t. Therefore, if $t \leq C$ the $\mathbf{y}_i$'s are decodable in their respective subcodes $(\mathcal{G}|V_{m_i})$. Hence $\mathbf{y}$ is decodable in $\mathcal{M}$. Moreover, even when $\text{Rk}(\mathbf{e}) > C$, it is sometimes possible to decode successfully. This corresponds to the case where $\text{Rk}(\mathbf{e}_i) \leq C$ for all $i = 1, \dots, u$.

We study occurrences of such case. We want to find an estimation of:

$$P_{decoding} = Pr(\text{Rk}(\mathbf{e_1}) \leq C, \dots, \text{Rk}(\mathbf{e_u}) \leq C) \mid \text{Rk}(\mathbf{e}) \leq t),$$

which quantifies the probability of successful decoding in $\mathcal{M}$.

Let $N = \sum_{i=1}^u m_i$, and let us consider the error-vector $\mathbf{e}$ as the q-ary $N \times n$ matrix corresponding to the expansion rowwise of the components of $\mathbf{e}$ on the basis of the N dimensional vector-space $V_{m_1} \oplus \cdots \oplus V_{m_u}$ with basis $(\mathbf{b}_1, \dots, \mathbf{b}_u)$. This gives the following representation for $\mathbf{e}$

$$\mathbf{e} = \begin{pmatrix} \mathbf{e_1} \\ \vdots \\ \mathbf{e_u} \end{pmatrix} \begin{array}{c} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_u \end{array}$$

where $\mathbf{e}_i$'s are q-ary matrices of size $m_i \times n$. We suppose that $\mathbf{e}^T$ is of rank $\leq t$, where t is some integer.

Matrix $\mathbf{e}^T$ can be transformed into a vector $\mathbf{E} = (\mathbf{E}_1 \cdots \mathbf{E}_u)$ with components in $GF(q^n)$ by considering any of its columns as the coordinates of an element of $GF(q^n)$ on a basis of $GF(q^n)/GF(q)$. This implies that $\mathrm{Rk}(\mathbf{E}) \leq t$ if and only if $\mathrm{Rk}(\mathbf{e}) \leq t$. In particular there exist $\alpha_1, \ldots, \alpha_t \in GF(q^n)^t$ linearly independent over $GF(q)$ satisfying

$$\mathbf{E} = (\alpha_1, \ldots, \alpha_t)S,$$

where S is a $t \times N$-matrix over $GF(q)$ of rank less than t. Consider the decomposition of $S = (S_1 \cdots S_u)$, where S_i are $t \times m_i$ q-ary matrices. We have

$$\begin{cases} \mathbf{E}_1 = (\alpha_1, \ldots, \alpha_t)S_1, \\ \vdots \\ \mathbf{E}_u = (\alpha_1, \ldots, \alpha_t)S_u. \end{cases}$$

Since the transformations from $\mathbf{e}_i$ to $\mathbf{E}_i$ are one-to-one and preserve the rank, and since the rank of $\mathbf{E}_i$ over $GF(q)$ is equal to the rank of S_i we have

$$P_{decoding} = Pr(\mathrm{Rk}(S_1) \leq C, \ldots, \mathrm{Rk}(S_u) \leq C) \mid \mathrm{Rk}(S) \leq t).$$

Matrix S being of size $t \times n$, the conditioning on the rank of S is always satisfied. Therefore we can remove it and we obtain

$$P_{decoding} = Pr(\mathrm{Rk}(S_1) \leq C, \ldots, \mathrm{Rk}(S_u) \leq C)).$$

The events being independent, this is equivalent to

$$P_{decoding} = Pr(\mathrm{Rk}(S_1) \leq C) \cdots Pr(\mathrm{Rk}(S_u) \leq C). \tag{2.11}$$

The number $\mathcal{N}_C(m,t)$ of $t \times m$ q-ary matrices of rank C is given by the formula, see [12] page 455 for instance:

$$\mathcal{N}_C(m,t) = \prod_{i=0}^{C-1} \frac{(q^m - q^i)(q^t - q^i)}{q^C - q^i}.$$

This quantity can be approximated by $q^{(m+t)C - C^2 + q^{-1} + O(q^{-2})}$, Therefore

$$Pr(\mathrm{Rk}(S_i) \leq C) = q^{(m_i - C)(C-t) + q^{-1} + O(q^{-2})}, \tag{2.12}$$

Hence from (2.11) and (2.12) we obtain

Proposition 4 (Probability of successful decoding)

Let $\mathcal{M} = (\mathcal{G}|V_{m_1}) \oplus \cdots \oplus (\mathcal{G}|V_{m_u})$, be the code formed by the direct sum of subspace subcodes of maximum rank distance codes with error-correcting capability C. Then the probability of success for decoding $t > C$ errors satisfies

$$P_{decoding} = q^{-(N-C)(t-C)+uq^{-1}+O(q^{-2})},$$

where $N = \sum_{i=1}^{u} m_i$.

3 A particular case: subfield subcodes

Subfield subcodes are special cases of subspace subcodes. In Hamming metric constructing a parity-check or generator matrix for these codes by using properties of the Trace operator is easy, [5, 9, 15]. What is less trivial is computing the exact dimension and exact minimum distance of the codes. Generally speaking, only bounds are available.

Section 2 showed that the exact parameters could be obtained very simply for the family of MRD-codes with parity-check matrix 1.2. Namely, subspace subcodes are isomorphic through a rank preserving bijection to MRD-codes of the same family but smaller parameters. This implies in particular that subspace subcodes are optimal for rank metric.

In this section we go one step further and show that, given a subfield $GF(q^s)$ of $GF(q^n)$ specified by a chosen basis, there is a unique subfield subcode modulo transformation by the group induced on the components of the code by the general linear group $GL_n(GF(q))$ of of q-ary non-singular matrices of size $n \times n$. We prove the following theorem.

Theorem 1

Let $\mathcal{G}$ be a code over $GF(q^n)$ with parity-check matrix (1.2), Let s be a positive integer dividing n and let

$$A = \begin{pmatrix} a_1 & \cdots & a_s \\ \vdots & \ddots & \vdots \\ a_1^{[d-2]} & \cdots & a_s^{[d-2]} \end{pmatrix}.$$

where the $a_i \in GF(q^s) \subset GF(q^n)$ for all $i = 1, \ldots, s$ are linearly independent over $GF(q)$.

Then, there exists a unique *matrix $S \in GL_n(GF(q))$ of size $n \times n$ such* *that the subfield subcode $(\mathcal{G}|GF(q^s))$ has parity-check matrix*

$$\mathbf{H}_{q^s} = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix} S,$$

Proof.

$\mathcal{G}$ has parity-check matrix (1.2) which can be rewritten

$$\mathbf{H} = \begin{pmatrix} \mathbf{h} \\ \vdots \\ \mathbf{h}^{[d-2]} \end{pmatrix}$$

where $\mathbf{h}^{[i]} \overset{def}{=} \left(h_1^{[i]}, \ldots, h_n^{[i]}\right)$. One obtains a parity-check matrix of $(\mathcal{G}|GF(q^s))$ by the following procedure:

- Choose a basis of $GF(q^n)/GF(q^s)$.
- Expand each line of matrix $\mathbf{H}$ onto $GF(q^s)$ with respect to this basis. Every line of length n with coefficients in $GF(q^n)$ is transformed columnwise into a matrix of size $n/s \times n$, that is

$$\mathbf{h} = (h_1, \ldots, h_n) \mapsto \mathcal{H} = \begin{pmatrix} h_{1,1} & \cdots & h_{1,n} \\ \vdots & \ddots & \vdots \\ h_{n/s,1} & \cdots & h_{n/s,n} \end{pmatrix};$$

However, since $\mathbf{H}$ is composed of lines obtained by the action of powers of the Frobenius automorphism on the components of $\mathbf{h}$, for all $i = 1, \ldots, d-2$, there exists a $n/s \times n/s$ non-singular matrix Q_i with coefficients in $GF(q^s)$ satisfying

$$\mathbf{h}^{[i]} = (h_1^{[i]}, \ldots, h_n^{[i]}) \mapsto Q_i \mathcal{H}^{[i]},$$

where $\mathcal{H}^{[i]}$ denotes matrix $\mathcal{H}$ whose components have been elevated to the power q^i. Therefore, a parity-check matrix of $(\mathcal{G}|GF(q^s))$ has the form

$$\mathbf{H}_{q^s} = \begin{pmatrix} \mathcal{H} \\ \mathcal{H}^{[1]} \\ \vdots \\ \mathcal{H}^{[d-2]} \end{pmatrix}$$

Next, since the columns of $\mathcal{H}$ have rank n over $GF(q)$ (the h_is are linearly independent over $GF(q)$), there is a $n \times n$ matrix S with coefficients in $GF(q)$ such that

$$\mathcal{H}S = \begin{pmatrix} \mathbf{a}_1 & 0 & \cdots & 0 \\ 0 & \mathbf{a}_2 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{a}_{n/s} \end{pmatrix},$$

where, for all $i = 0, \ldots, d-2$

$$\mathbf{a}_i = (a_{i,1}, \ldots, a_{i,s}), \quad a_{i,j} \in GF(q^s)$$

is a vector formed with linearly independent elements of $GF(q^s)$. Provided $d - 2 < s$ the following matrices

$$\mathcal{A}_i = \begin{pmatrix} \mathbf{a}_i \\ \vdots \\ \mathbf{a}_i^{[d-2]} \end{pmatrix}, \quad \text{for } i = 1, \ldots, n/s$$

are generator matrices of a $[s, s-d+1, d]$ MRD-code over $GF(q^s)$. This implies the existence of a permutation matrix P such that

$$\mathbf{H}_{q^s} = \begin{pmatrix} \mathcal{H} \\ \mathcal{H}^{[1]} \\ \vdots \\ \mathcal{H}^{[d-2]} \end{pmatrix} = P \begin{pmatrix} \mathcal{A}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathcal{A}_{n/s} \end{pmatrix} S^{-1}$$

To complete the proof we have to remark that, multiplying a parity-check matrix on the left by any non-singular matrix doesn't change the generated code. Hence a parity-check of $(\mathcal{G}|GF(q^s))$ is

$$\begin{pmatrix} \mathcal{A}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathcal{A}_{n/s} \end{pmatrix} S$$

If $A \overset{def}{=} \mathcal{A}_1$, for all $i = 1, \ldots, n/s$ there exists a non-singular matrix P_i over $GF(q^s)$ such that $\mathcal{A}_i = P_i \mathcal{A}$. Hence

$$\begin{pmatrix} \mathcal{A}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathcal{A}_{n/s} \end{pmatrix} = \begin{pmatrix} P_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & P_{n/s} \end{pmatrix} \begin{pmatrix} A & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A \end{pmatrix},$$

and a parity-check matrix of $(\mathcal{C}|GF(q^s))$ is

$$\mathbf{H}_{q^s} = \begin{pmatrix} A & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A \end{pmatrix} S.$$

This completes the proof.

The theorem means that, somehow, the subfield subcode of a maximum rank distance code of full length (*i.e.* the length of the code is equal to the extension degree) is a direct sum of maximum rank distance codes taken over the subfield.

It also implies that, whatever the MRD-code over $GF(q^n)$ be, if we fix a basis of $GF(q^n)/GF(q^s)$, then the subfield subcode is uniquely determined by a q-ary invertible matrix S.

From proposition 4 we deduce the following corollary

Corollary 3 (Successful decoding of subfield subcodes)

Let C be the error-correcting capability of $\mathcal{G}$, then the probability of decoding $t > C$ errors in $(\mathcal{G}|GF(q^s))$ is equal to

$$P_{decoding} = q^{-(n-C)(t-C)+\frac{n}{s}q^{-1}+O(q^{-2})},$$

References

[1] J. Bierbrauer and Y. Edel. New code parameters from Reed-Solomon subfield subcodes. *IEEE Transactions on Information Theory*, 43(3):953–968, May 1997.

[2] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.

[3] F. Chabaud and J. Stern. The cryptographic security of the syndrome decoding problem for rank distance codes. In K. Kim and T. Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '96*, volume 1163 of *LNCS*. Springer-Verlag, November 1996.

[4] K. Chen. A new identification algorithm. In *Cryptographic policy and algorithms*, volume 1029, pages 244–249. Springer, 1996.

[5] P. Delsarte. On subfield subcodes of modified Reed–Solomon codes. *IEEE Transactions on Information Theory*, 20:575–576, 1975.

[6] E. M. Gabidulin. Theory of codes with maximal rank distance. *Problems of Information Transmission*, 21:1–12, July 1985.

[7] E. M. Gabidulin. A fast matrix decoding algorithm for rank-error correcting codes. In G. Cohen, S. Litsyn, A. Lobstein, and G. Zémor, editors, *Algebraic coding*, volume 573 of *LNCS*, pages 126–133. Springer-Verlag, 1991.

[8] E .M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In D. .W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, volume 547 of *LNCS*, pages 482–489. Springer-Verlag, 1991.

[9] V. D. Goppa. A new class of linear error-correcting codes. *Problems of Information Transmission*, 6(3):207–212, 1970.

[10] M. Hattori, R. J. McEliece, and G. Solomon. Subspace subcodes of Reed–Solomon codes. *IEEE Transactions on Information Theory*, 44(5), September 1998.

[11] J. M. Jensen. Subgroup subcodes. *IEEE Transactions on Information Theory*, 41(3):781–785, May 1995.

[12] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, 2nd edition, 1997.

[13] P. Loidreau. A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In *Proceedings of the 4th International Workshop on Coding and Cryptography, WCC 2005.*

[14] P. Loidreau. Sur la reconstruction des polynômes linéaires : un nouvel algorithme de décodage des codes de Gabidulin. *Comptes Rendus de l'Académie des Sciences : Série I*, 339(10):745–750, 2004.

[15] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error–Correcting Codes*, chapter 12. North Holland, 1977.

[16] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab. DSN Progress Report, 1978.

[17] R. J. McEliece and G. Solomon. Trace-shortened Reed–Solomon codes. Technical Report 42-117, TDA Progress Report, May 1994.

[18] A. Ourivski and T. Johannson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38(3):237–246, September 2002.

[19] A. V. Ourivski, E. M. Gabidulin, B. Honary, and B. Ammar. Reducible rank codes and their applications to cryptography. *IEEE Transactions on Information Theory*, 49(12):3289–3293, December 2003.

[20] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *Proceedings of ISIT 2004*, 2004.

[21] R. M. Roth. Maximum-Rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, March 1991.

[22] G. Solomon. Nonlinear, nonbinary cyclic group codes. Technical Report 42-108, TDA Progress Report, February 1992.

[23] H. Stichtenoth. On the dimension of subfield subcodes. *IEEE Transactions on Information Theory*, 36, 1990.

[24] M. van Dijk and L. Tolhuizen. Efficient encoding for a class of subspace subcodes. *IEEE Transactions on Information Theory*, 45(6):2142–2146, 1999.